IN THE DISCLOSURE:

Please amend the three paragraphs starting on page 4, line 1 and ending on page 4, line 8 as follows:

-- An advantage ~~second object~~ of the present invention is that several institutions could use the same apparatus to significantly reduce the implementation costs associated therewith.

Another advantage ~~object~~ of the present invention is that a same apparatus can provide all variable identification codes (VIC) for the user to become formally identified with several adherent organizations during transactions therewith.

Another advantage ~~object~~ of the present invention is that the method does not require the installation of new terminals and functions with the already existing ones. –

Please delete the seven paragraphs of the "Summary of the Invention" Section starting on page 4, line 10 and ending on page 6, line 10 and add the following new paragraphs:

-- According to an aspect of the present invention, there is provided a universal identification device for providing a user first party with a variable identification code required for a transaction with a predetermined service provider second party to be validated, said device comprises: a second party selection unit for selecting said predetermined second party from a plurality of second parties; a data input unit for receiving a user identification code from said first party; a data processing unit connected to said second party selection unit and said data input unit, said data processing unit processing said user identification code and said predetermined second party to generate said variable identification code required for said transaction to be validated; and a data output unit connected to said data processing unit for receiving said variable identification code therefrom, said data output unit providing said variable identification code to said first party.

Typically, the data processing unit includes a memory member having at least one second party key code corresponding to said predetermined second party stored therein, said data processing unit processing said user identification code and said at least one second party key code to generate said variable identification code required for said transaction to be validated.

In one embodiment, the data processing unit processes said user identification code and said at least one second party key code through an algorithm to generate said variable identification code required for said transaction to be validated.

Typically, the second party selection unit includes a selection keypad, said selection keypad having a plurality of party keys, each of said plurality of party keys being assigned to a respective said plurality of second parties.

In one embodiment, the device includes a keypad, said keypad being connected to at least one of said second party selection unit and said data input unit.

Typically, the keypad includes at least one selection key, at least one validation key and at least one deletion key; and the data output unit includes a visual display. The visual display is connected to said second party selection unit, said at least one selection key allowing said visual display to successively display said plurality of second parties, said at least one validation key allowing selection of said second party being displayed.

In one embodiment, the visual display is connected to said keypad so as to allow said first party to enter a sequence of selected characters via said at least one selection key and without using character-identified keys, said visual display preventing display of said sequence of selected characters.

In one embodiment, the visual display includes a plurality of printed characters thereon and a displaceable cursor to successively face said plurality of printed characters, said visual display being connected to said keypad for cooperation therewith.

Typically, the at least one selection key is a selection scrolling key, said selection scrolling key displacing said cursor for selection of successive figures corresponding to respective said plurality of printed characters, each said successive figures being selected by said user party using said at least one validation key when said cursor successively faces respective said plurality of printed characters, said successive figures forming data to be entered within said device.

In one embodiment, the cursor is randomly positioned after selection of respective said plurality of printed characters using said at least one validation key.

In one embodiment, the data input unit includes a microphone connected to said data output unit so as to be usable as a speaker when connected thereto.

Typically, the microphone is connected to said second party selection unit so as to allow said first party to verbally select said predetermined second party from said plurality of second parties.

In one embodiment, the data input unit includes a biometric data reader. Typically, the biometric data reader includes a fingerprint reader, or includes a microphone so as to allow voice recognition for voiceprint input.

In one embodiment, the memory member has first and second second party key codes corresponding to each of said plurality of second parties stored therein, said data processing unit processing said user identification code and said first and second second party key codes corresponding to said predetermined second party to generate said variable identification code required for said transaction to be validated.

Typically, the first and second second party key codes are stored in said memory member by said first party at registration of corresponding said plurality of second parties.

In one embodiment, the memory member includes a reference user code stored therein, said algorithm including: a) obtaining data of said predetermined second party from said second party selection unit; b) obtaining data of said user

identification code from said data input unit; c) comparing said user identification code with said reference user code, returning to step b) when said user identification code is different than said reference user code, and resuming when said user identification code is identical to said reference user code; d) calculating said variable identification code using at least said at least one second party key code; and e) providing said variable identification code to said data output unit.

Typically, the memory member includes a predetermined combination table data stored therein, said algorithm calculating said variable identification code using said at least one second party key code and eventually at least part of said user identification code to modify one of a successive combination of said predetermined combination table data.

In one embodiment, the data output unit is connectable to a terminal so as to communicate said variable identification code thereto. Typically, the device is a chip card having a chip therein connectable to the terminal, said data output unit connecting to said chip for communication of said variable identification code to the terminal.

According to another aspect of the present invention, there is provided a method for providing a user first party with a variable identification code using a universal identification device, said variable identification code being required for a transaction with a predetermined service provider second party to be validated, said method comprises: a) selecting said predetermined second party from a plurality of second parties registered within said device; b) receiving a user identification code from said first party; c) processing said user identification code and said predetermined second party to generate said variable identification code required for said transaction to be validated; and d) providing said variable identification code to said first party.

In one embodiment, the device includes at least one second party key code corresponding to said predetermined second party stored therein, said processing

step c) including processing said user identification code and said at least one second party key code to generate said variable identification code required for said transaction to be validated.

Typically, the device includes a reference user code stored therein, said processing step c) including: c1) comparing said user identification code with said reference user code; c2) returning to said receiving step b) when said user identification code is different than said reference user code; c3) generating said variable identification code required for said transaction to be validated when said user identification code is identical to said reference user code.

In one embodiment, the device is turned off after a predetermined amount of successive returning to said receiving step b) when successive said user identification codes are different from said reference user code.

In one embodiment, the reference user code is a biometric data of said first party.

Typically, the reference user code is known to said device only so as to remain confidential thereto without being communicated to said plurality of second parties or to a third party.

In one embodiment, the method further includes, before said selecting step a), the step of: registering said plurality of second parties within said device.

Typically, the registering step a) includes: storing at least one second party key code for respective each said plurality of second parties within said device. The processing step c) includes: processing said user identification code and said at least one second party key code through an algorithm to generate said variable identification code required for said transaction to be validated.

Typically, the storing step includes: storing two second party key codes for respective each said plurality of second parties within said device.

In one embodiment, the device includes a reference user code stored therein, said algorithm including: c1) obtaining data of said predetermined second party and said

user identification code; c2) comparing said user identification code with said reference user code, returning to said receiving step b) when said user identification code is different than said reference user code, and resuming when said user identification code is identical to said reference user code; and c3) calculating said variable identification code using at least said at least one second party key code.

Typically, the device includes a predetermined combination table data stored therein, said algorithm calculating said variable identification code using said at least one second party key code and eventually at least part of said user identification code to modify one of a successive combination of said predetermined combination table data.

In one embodiment, the method further includes: e) communicating said variable identification code to said predetermined second party; f) analyzing said communicated variable identification code to verify identity of said first party so as to validate the transaction.

Typically, the analyzing step f) includes comparing said communicated variable identification code to a list of predetermined codes.

Alternatively, the device includes at least one second party key code corresponding to said predetermined second party stored therein, said processing step c) including processing said user identification code and said at least one second party key code to generate said variable identification code, and said analyzing step f) including calculating at least one identification code through an algorithm using at least part of said user identification code and said at least one second party key code. --

Please amend the twelve paragraphs starting on page 7, line 19 and ending on page 12, line 12 as follows:

-- Referring to figure 1, we see that the apparatus or device (1) consists of a case ~~case (1)~~ the size of a traditional ID card but slightly thicker which includes a data processing unit including a microprocessor (14), an energy source (not shown)

which can be a battery or a solar energy collector. The case can be rectangular in shape as seen in figure 1 or have any other shape. The case includes a display screen (2), figures or characters (3) 1,2,3,4,5,6,7,8,9,0 printed around the visual screen (2) and five keys (4,5,6,7,8) which are as follows: A key (6) bearing the inscription "power" being used to activate the apparatus (1); A key (7) bearing the inscription "enter" used for validation and the recording of data; A key (8) bearing the inscription "clear" used for the cancellation or deletion of the last validated data; A key (5) bearing an arrow icon used to move the cursor (9) to the right of the screen (2); A key (4) bearing an arrow icon used to move the cursor (9) to the left of the screen (2);

The drawing in figure 2 represents another model of the apparatus (1). In this model the identification of the holder is not made by entering a PIN but rather by the reading of a fingerprint. For that purpose a mini fingerprint reader (11) is integrated on the surface of the apparatus (1). The microprocessor (14) records the digitized fingerprint of its holder during the initial activation of the apparatus (1). Afterwards, the identification of the holder is made by comparing (72) the digitized fingerprint of the finger that is placed on the mini reader (11) to the one in the memory member of the microprocessor (14) of the apparatus (1). If they are identical, then the apparatus displays (67, 75) the VIC (10) for the desired file.

The drawing in figure 3 represents a model of the apparatus (1) which is comparable to that of figure 1. The difference being with the integration of a supplementary keypad (12) which allows to directly choose a file from among those which were activated beforehand by hitting on the appropriate key (12).

The drawing in figure 4 represents an apparatus (1) which does not contain a secured keypad (4, 5) but instead, a standard character-identified or numerical keypad (13). This apparatus (1) is also provided with a keypad (12) allowing to directly choose the file from the ones which were activated beforehand by hitting the appropriate key (12).

The drawing in figure 5 represents an apparatus (1) with a transducer (15) serving as a microphone or speaker, hence for the input and output of data. It is activated by hitting the key (16). The apparatus (1) will be in data input mode when the talk key (16) is pressed down, the input of data is made verbally by the user. The output of data is also made verbally via the speaker when the key (16) is not being pressed down.

Figure 6 represents a functional diagram of the apparatuses (1) working on the identification of the card holder, or user first party, through the use of a user identification code such as a PIN (figs.1,3,4). The apparatus (1) is turned on by hitting (51) the "power" key (6) to begin a use (61). The holder chooses the adherent organization (62), or service provider second party, then enters his PIN (63). The microprocessor (14) compares (64) the PIN entered with the PIN in the memory (14) used as a reference user code. If the PIN entered is different from the memorized PIN (68) then the apparatus (1) requests reentry (63) of the PIN. After three unsuccessful attempts, the apparatus (1) shuts down. In order to reactivate the apparatus (1) the holder has to enter a special code supplied by the adherent organization. If the entered PIN is identical (65) to the memorized PIN then the microprocessor (14) generates a variable identification code (VIC) (10) specific to the current use by using the entered PIN (63), at least one second party key code, preferably two such as a reference code (82) and a validation code (83) characteristic of the adherent organization to modify a combination extracted from a table of combinations integrated into the apparatus (1). The variable identification code (VIC) (10) is revealed (67) by means of the data output device or unit (2). The end user hits (52) the "power" key (6) to terminate use and turn off (69) the apparatus (1).

Figure 7 represents a functional diagram of the apparatuses (1) working on the identification of the holder by the supply of biometric data (figs.2 and 5). The apparatus (1) is turned on by hitting (51) the "power" key (6 or 16) to begin a use (61). The holder chooses the adherent organization (62) then provides a biometric

data (71). The microprocessor (14) compares the data with the one in memory (14) used as a reference user code. If the entered biometric data (71) is different from that the reference memorized one (74) then the apparatus (1) requests reentry (71) of the biometric data. After three unsuccessful attempts, the apparatus (1) shuts down. In order to reactivate the apparatus (1) the holder has to enter a special code supplied by the adherent organization. If the entered biometric data is identical (73) to the memorized one, the microprocessor (14) then generates (75) a variable identification code (VIC)(10) specific to the current use by using a reference code (82) and a validation code (83) characteristic of the adherent organization to modify a combination extracted from a combination table ~~of combinations~~ integrated into the apparatus (1). The variable identification code (VIC) (10) is revealed (67) by means of the data output device (2,15). The end user hits (52) the "power" key (6) to terminate the use and turn off (69) the apparatus (1).

Figure 8 represents a block diagram illustrating the steps needed at the registration of an adherent organization to open a file (80) up to the transmission (89) of a variable identification code (VIC) (10) for apparatuses (1) (figs.1,3 and 4) identifying the holder by the supplying (63) of a PIN. To open a file with an adherent organization, the holder of the apparatus (1) registers (81) a personal identification number (PIN) with the organization. The organization issues a reference code (82) and a validation code (83) characteristic of this organization for this end-user. The holder of the apparatus (1) then activates a file in his apparatus (1) for this organization. He gives (84) it an identification character then records (84.1) his corresponding personal identification number (PIN). He records (85) in his apparatus (1) the reference code (82) and the validation code (83) characteristic of the organization. To obtain a variable identification code (VIC) (10) the holder must select (86) with his apparatus (1) an adherent organization, enter his PIN (87). In this way he obtains (88) from his apparatus (1) a variable identification code (VIC) (10). He then communicates (89) this variable identification code (VIC) (10) to the adherent organization to allow the latter to verify his identity.

Figure 9 represents a block diagram illustrating the steps needed to open a file (90) up to the transmission (89) of a variable identification code (VIC) (10) for apparatuses (1) (figs. 2 and 5) identifying the holder by the supplying (71) of biometric data. To open a file with an adherent organization, this organization issues a reference code (82) and a validation code (83) characteristic of this organization for this end-user. The holder activates a file in his apparatus (1) for this organization by giving (84) it an identification character. Then he records (91) a biometric data as a reference user code. Next, he records (85) the reference code (82) and the validation code (83) characteristic of this organization in his apparatus (1). In order to obtain a variable identification code (VIC)(10) the holder must, by means of his apparatus (1), select (86) an adherent organization, enter (92) a biometric data. In this way he obtains (88) from his apparatus (1) a variable identification code (VIC) (10). He then communicates (89) this variable identification code (VIC) (10) to the adherent organization to allow the latter to verify his identity.

Figure 10 represents a flow diagram of the general flow (100) of an identification process. The holder must first turn on (101) his apparatus (1), select (86) and validate (102) an adherent organization using a second party selection unit via the data input device or unit (4, 5, 7, 8, 11, 12, 13, 15). According to the model of apparatus (1) he holds, he must (figs.1, 3 and 4) enter (103) and validate (104) his PIN, or for the apparatuses of figures 2 and 5 enter (92) a biometric data by means of the appropriate device (11 and 15). After validation (65 or 73), the apparatus (1) provides (88) a variable identification code (VIC) (10). The user communicates (89) this VIC (10) to the adherent organization. The latter analyzes (105) the VIC, if the provided (89) VIC (10) is valid (106) the identification of the holder by the adherent organization is then validated (108). If the transmitted (89) VIC (10) is erroneous (107) the adherent organization then rejects the identification of the holder.

Figure 11 is a simplified schematic demonstrating a procedure of authorization according to the present invention for a commercial transaction with a payment card. The holder of the apparatus (1) brings the intended purchase to the cashier. Having

decided to pay the purchase price with his payment card, he offers it to the cashier. The cashier enters the necessary details into the cash register such as the purchase amount then swipes as usual the card through the magnetic card reader to establish the communication (111). The communication takes place with current protocols. The adherent organization verifies (112) the validity of this information and when validated (113) the transaction can continue, otherwise (114) the transaction is cancelled (116). Once this step is over, the financial institution that issued the payment card asks (115) the variable identification code (VIC) (10) from the holder. The holder, by means of his apparatus (1) gets (115) a variable identification code (VIC) (10) and transmits (89) this (VIC) (10) to the adherent organization which validates (105) it. If it is erroneous (107), the transaction is cancelled (118). If the transmitted (89) VIC (10) is valid (106) then the transaction is authorized.

The apparatus (1) and the method (100) are dedicated to the identification of its holder in the course of approaches undertaken with organizations that has adhered to this service. The identification is made by means of a code called "variable identification code (VIC (10)". This code is unique and different for each use. It is valid for a single transaction then replaced by another VIC (10) for a subsequent use. The variable identification code (VIC) (10) is supplied by the apparatus (1) and revealed (67) to its holder by means of the data output device (2,15). The same apparatus (1) serves to identify its holder in various situations of everyday life such as interactions with his employer, the government, transactions using a payment card (credit or debit) or transaction with any other adherent organization. Accordingly, the apparatus (1) processes several files that could be allocated (84) to different organizations or service providers by its holder. –

Please amend the first full paragraph of page 14 as follows:

-- According to the preferred method, there is provided the general functioning of the algorithm, there exists in all apparatuses a basic combination table consisting of 10 rows. Each of these rows consists of a 12-figure code or combination. This

basic table is present 5 times in apparatuses able to handle 5 files and 15 times for apparatuses able to handle 15 files etc. Each of the files works independently of the other files. --

Please amend the five paragraphs starting on page 16, line 30 and ending on page 18, line 12 as follows:

-- How does the secured (non-character-identified) keypad (4, 5, 6, 7, 8) (figs.1, 2 et 3). As opposed to the existing approaches, the keypad (4, 5, 6, 7, 8) used to record (84.1, 85) the essential data (reference code (82), validation code (83) provided by the adherent organization, PIN etc.) inside the apparatus (1) is not numerical. This secured keypad (4, 5, 6, 7, 8) is another innovation of this apparatus (1). It includes mainly two keys identified by arrows (4, 5). These keys (arrows) (4,5) are used to scroll a cursor (9) appearing on the screen (2) of the apparatus (1). A key (arrow)(4) for displacing the cursor (9) to the left and another key (arrow) (5) for displacing it to the right.

Obviously, there are other keys on the apparatus (1). These other keys are respectively: "power"(6) to activate of the apparatus (1), "ENTER"(7) to validate and record an entry and "CLEAR"(8) to cancel the last entry. Lets look at how the keys (4,5) of the apparatus (1) make the transaction much safer.

A user has already activated a file in his apparatus (1). He is with a retailer and wants to carry out a transaction. He turns on the apparatus (1) by hitting (51) the "power"(6) key. Then the inscription "file No." appears on the screen (2) with a cursor (9) under the character (3) 1. Since the user has only one activated file (adherent organization) in his apparatus (1), he immediately presses down the "ENTER"(7) key to confirm that he wants to get a variable identification code (VIC) (10) for the file No. 1. Then the inscription "PIN" and a cursor (9) appear on the screen (2) of the apparatus (1). This cursor (9) successively faces the characters (3) by being typically located ~~is located~~ under or above one of the characters (3) printed around the screen (2): "1 2 3 4 5 6 7 8 9 0"(3). For maximum security the cursor(9)

never appears under or above the same character (3). It may appear under the character 1 and the next time reappear, in a random fashion, under the character 5 or above the character 8 etc.

For the purpose of our example, the PIN of the user is 6384. The cursor (9) appeared under the character (3) 2. Since the first digit of the PIN is 6, the user hits four times the right arrow(5) to move the cursor (9) above the character (3) 6. Then he hits the "ENTER"(7) key to validate and record this first digit.

The cursor (9) momentarily disappears from the screen (2) and reappears under or above another character (3), this character (3) being randomly selected again. At the same time, a symbol such as this one: "*" appears on the screen (2) to indicate that the first digit of the PIN has been selected. Obviously this symbol "*" will appear twice to indicate that the first two digits of the PIN have been selected, and so on. Resuming to our example, this time the cursor(9) reappears above the character 9. T he user then hits six times on the left arrow (4) to move the cursor(9) under the character(3) 3. Since the second digit of his PIN is really the 3, he hits the "ENTER"(7) key to validate and record this digit. The same process starts over for the selection of the third and fourth digits of his PIN. In the case he would have made an error by hitting the "ENTER"(7) key too rapidly, he could have hit the "CLEAR"(8) key to cancel or delete the last entry, make the correction and resume. The cursor is located at the top of the screen(2) for the characters (3) 1,2,3,4,5 and at the bottom of the screen (2) for the characters (3) 6,7,8,9,0. –